ASA/PIX:CLI 및 ASDM 컨피그레이션을 사용하는 VPN 클라이언트 트래픽용 인바운드 NAT가 있는 원격 VPN 서버 예

목차

소개

이 문서에서는 Cisco 5500 Series ASA(Adaptive Security Appliance)가 ASDM(Adaptive Security Device Manager) 또는 CLI 및 NAT를 사용하여 인바운드 VPN 클라이언트 트래픽을 사용하여 원격 VPN 서버로 작동하도록 구성하는 방법에 대해 설명합니다.ASDM은 직관적이고 사용하기 쉬운 웹 기반 관리 인터페이스를 통해 세계적인 수준의 보안 관리 및 모니터링을 제공합니다.Cisco ASA 컨피그레이션이 완료되면 Cisco VPN 클라이언트를 통해 확인할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에서는 ASA가 완전히 작동 중이고 Cisco ASDM 또는 CLI에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.ASA는 아웃바운드 NAT에 대해서도 구성된 것으로 간주됩니다.아웃바운드 NAT 구성 방법에 대한 자세한 내용은 PAT를 사용하여 내부 호스트가 외부 네트워크에 액세스하도록 허용을 참조하십시오.

참고: ASDM 또는 PIX/ASA 7.x에 대한 HTTPS 액세스 허용을 참조하십시오.ASDM 또는 SSH(Secure Shell)에서 디바이스를 원격으로 구성할 수 있도록 하려면 Inside 및 Outside Interface

Configuration Example의 SSH를 사용합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 7.x 이상
- Adaptive Security Device Manager 버전 5.x 이상
- Cisco VPN Client 버전 4.x 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 Cisco PIX Security Appliance 버전 7.x 이상에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

원격 액세스 컨피그레이션은 모바일 사용자와 같은 Cisco VPN 클라이언트에 안전한 원격 액세스를 제공합니다.원격 액세스 VPN을 사용하면 원격 사용자가 중앙 집중식 네트워크 리소스에 안전하게 액세스할 수 있습니다.Cisco VPN Client는 IPSec 프로토콜을 준수하며 보안 어플라이언스와 작동하도록 특별히 설계되었습니다.그러나 보안 어플라이언스는 많은 프로토콜 호환 클라이언트와의 IPSec 연결을 설정할 수 있습니다.IPSec에 대한 자세한 내용은 ASA 컨피그레이션 가이드를 참조하십시오.

그룹과 사용자는 VPN 보안 관리 및 보안 어플라이언스 컨피그레이션의 핵심 개념입니다.VPN에 대한 사용자 액세스 및 VPN 사용을 결정하는 특성을 지정합니다.그룹은 단일 엔티티로 처리되는 사용자 모음입니다.사용자는 그룹 정책에서 특성을 가져옵니다.터널 그룹은 특정 연결에 대한 그룹 정책을 식별합니다.사용자에게 특정 그룹 정책을 할당하지 않으면 연결에 대한 기본 그룹 정책이 적용됩니다.

터널 그룹은 터널 연결 정책을 결정하는 레코드 집합으로 구성됩니다.이러한 레코드는 터널 사용자가 인증되는 서버와 연결 정보가 전송되는 어카운팅 서버(있는 경우)를 식별합니다.또한 연결에 대한 기본 그룹 정책을 식별하고 프로토콜별 연결 매개변수를 포함합니다.터널 그룹에는 터널 자체의 생성과 관련된 소수의 특성이 포함됩니다.터널 그룹에는 사용자 지향 특성을 정의하는 그룹 정책에 대한 포인터가 포함됩니다.

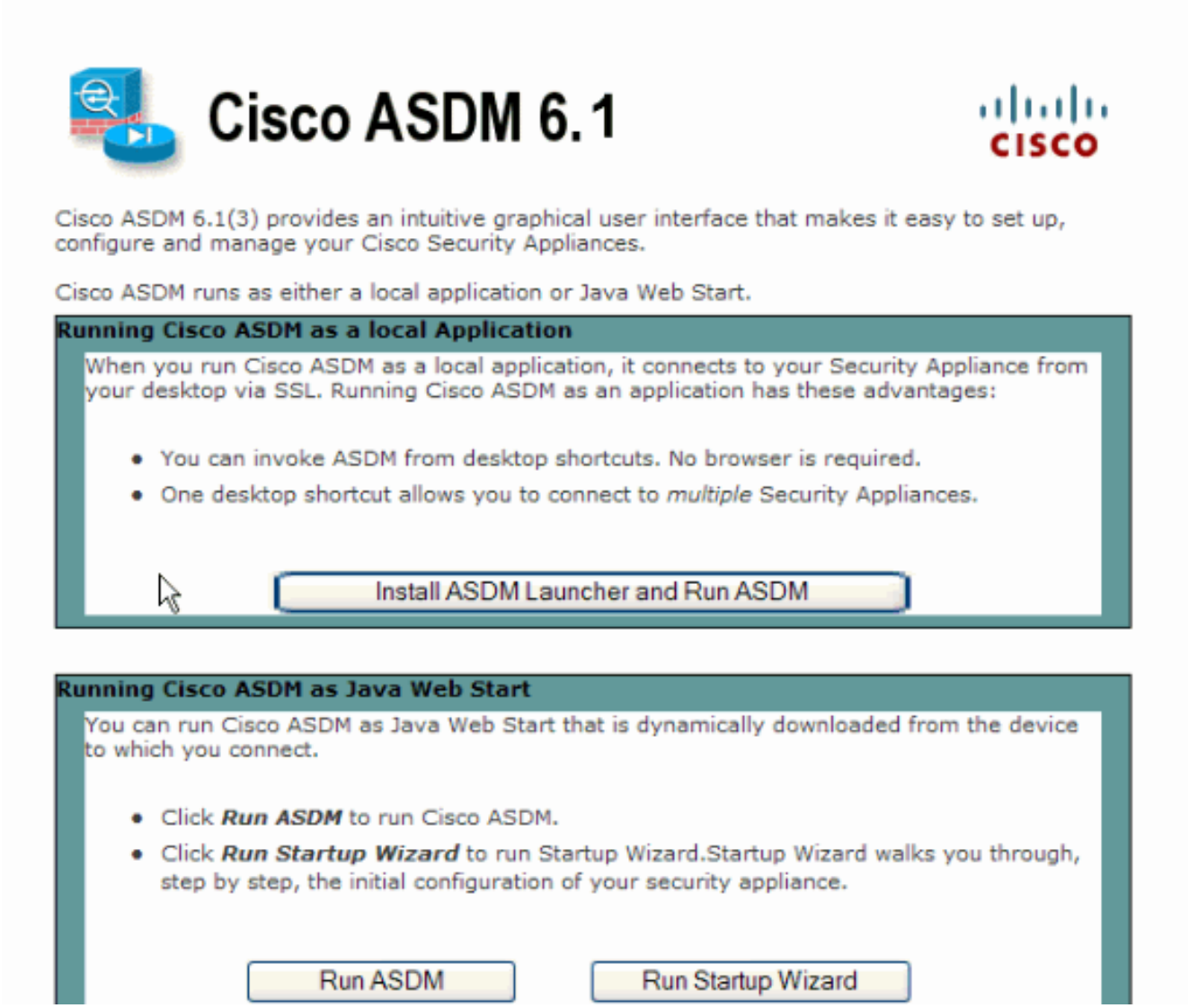
구성

ASDM을 사용하여 ASA/PIX를 원격 VPN 서버로 구성

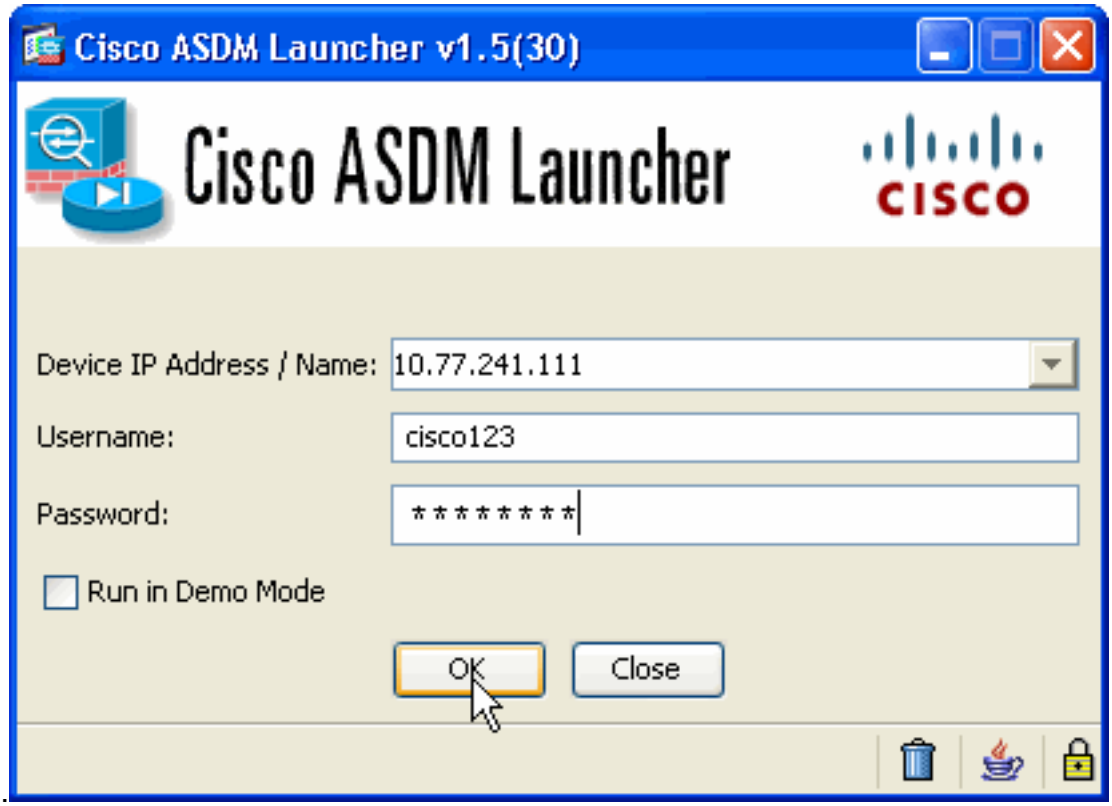
ASDM을 사용하여 Cisco ASA를 원격 VPN 서버로 구성하려면 다음 단계를 완료합니다.

1. 브라우저를 열고 **ASA의 ASDM에** 액세스하려면 **https://<IP_Address of ASA interface that has configured for ASDM Access>**를 입력합니다.브라우저에서 SSL 인증서 신뢰성과 관련된 경고를 승인해야 합니다.기본 사용자 이름과 비밀번호는 모두 비어 있습니다.ASA는 ASDM 애플리케이션을 다운로드할 수 있도록 이 창을 표시합니다.이 예에서는 응용 프로그램을 로컬 컴퓨터에 로드하며 Java 애플릿에서 실행되지 않습니다

.

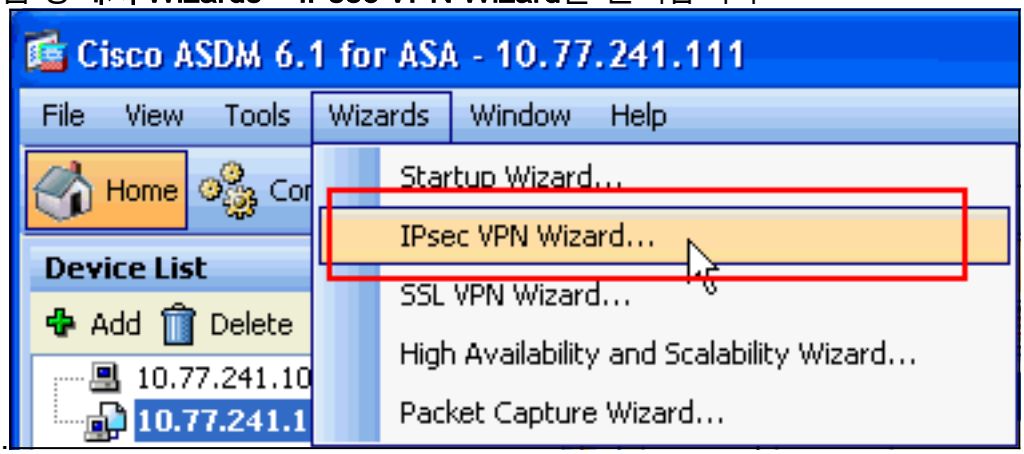


2. ASDM 애플리케이션 **설치** 프로그램을 다운로드하려면 **Download ASDM Launcher and Start ASDM(ASDM 시작** 시작 **시작**)을 클릭합니다.
3. ASDM Launcher가 다운로드되면, 소프트웨어를 설치하고 Cisco ASDM Launcher를 실행하기 위해 프롬프트에 의해 지시된 단계를 완료합니다.
4. **http -** 명령으로 구성한 인터페이스의 IP 주소를 입력하고 사용자 이름과 비밀번호를 지정한 경우 입력합니다.이 예에서는 **cisco123**을 사용자 이름으로, **cisco123**을 비밀번호로 사용합니



다.

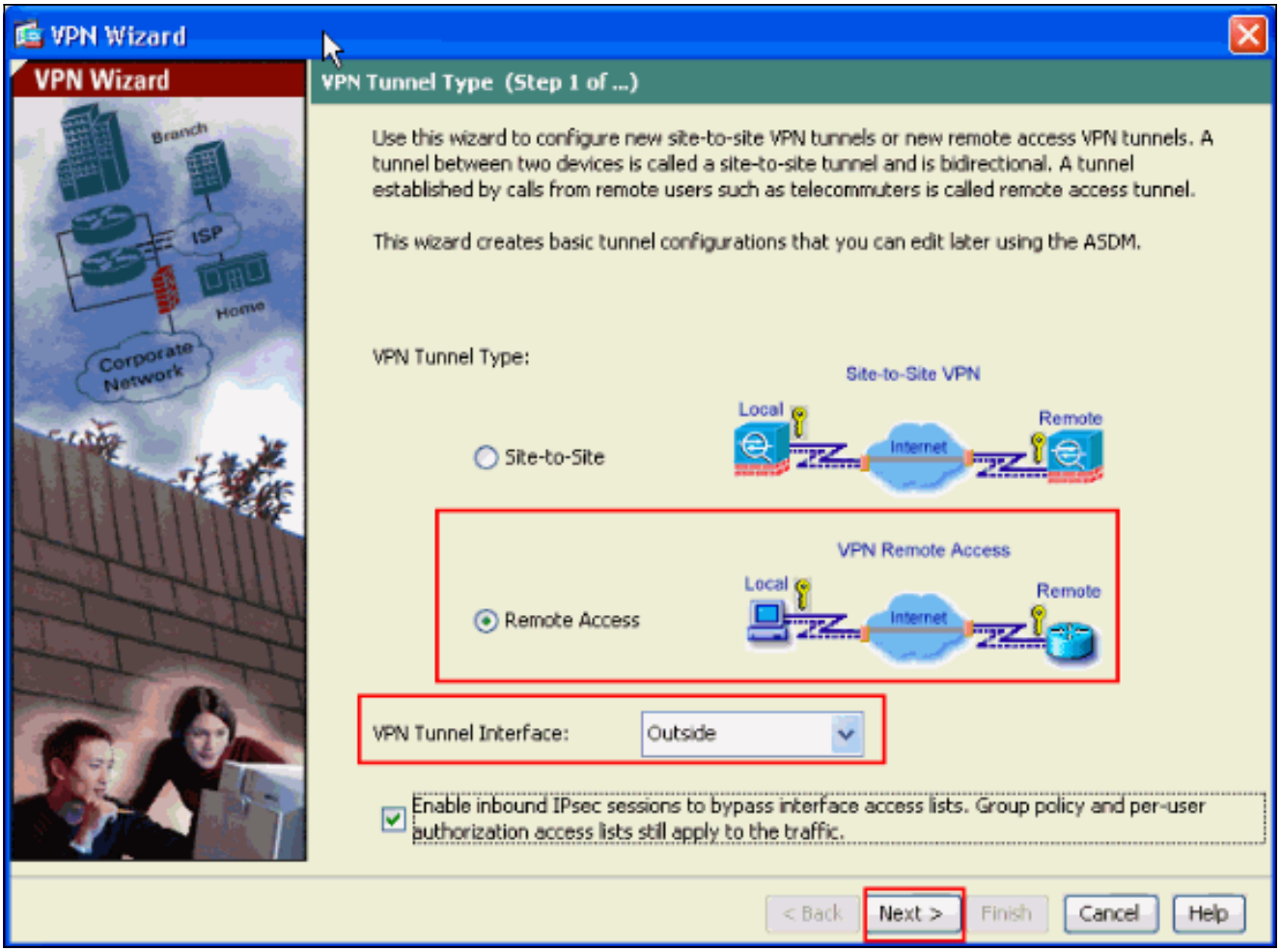
5. 홈 창에서 **Wizards > IPsec VPN Wizard**를 선택합니다



.

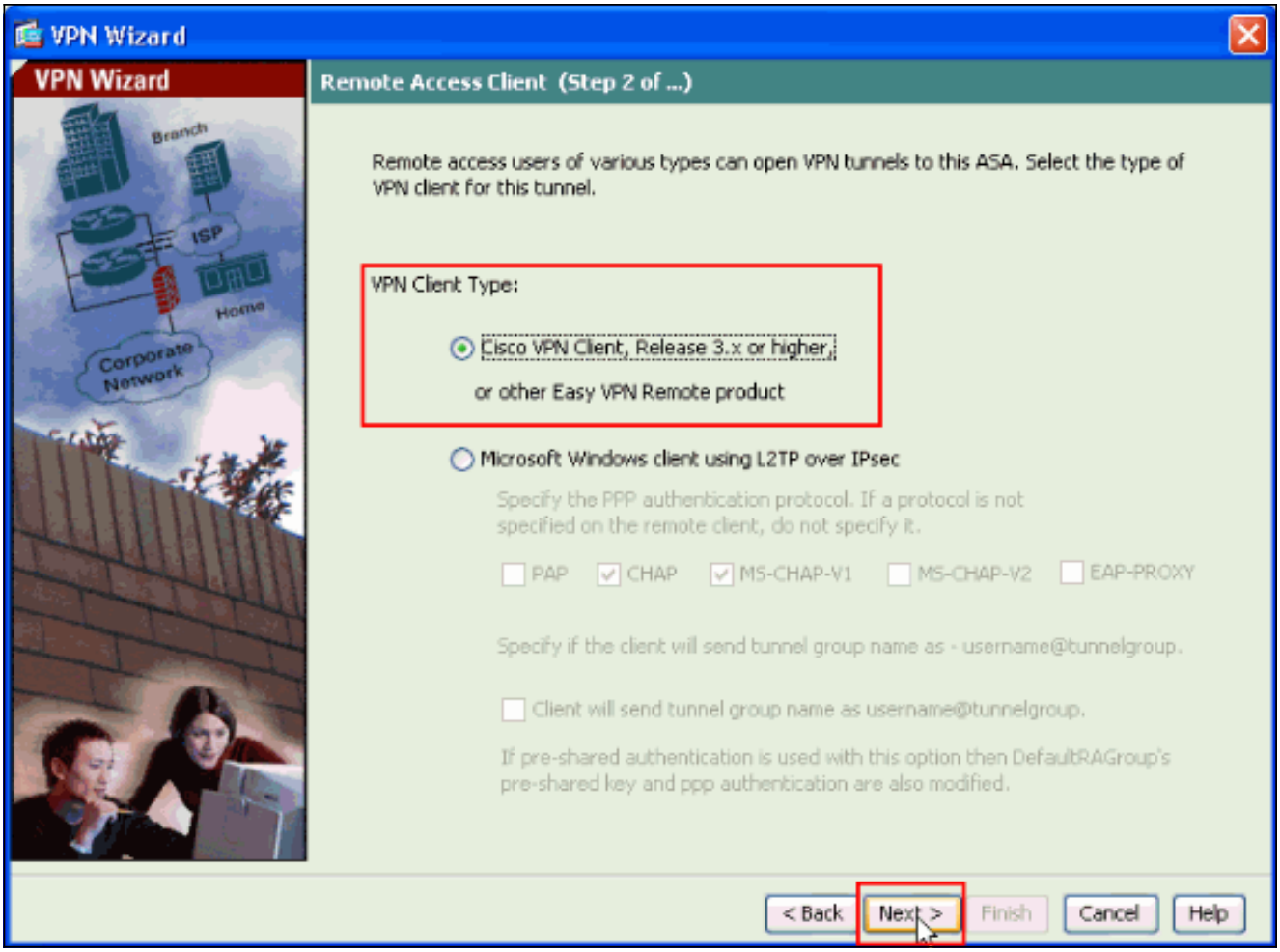
6. Remote **Access** VPN 터널 유형을 선택하고 VPN 터널 인터페이스가 원하는 대로 설정되었는지 확인한 다음 여기**와** 같이 Next(**다음)를** 클릭합니다

.



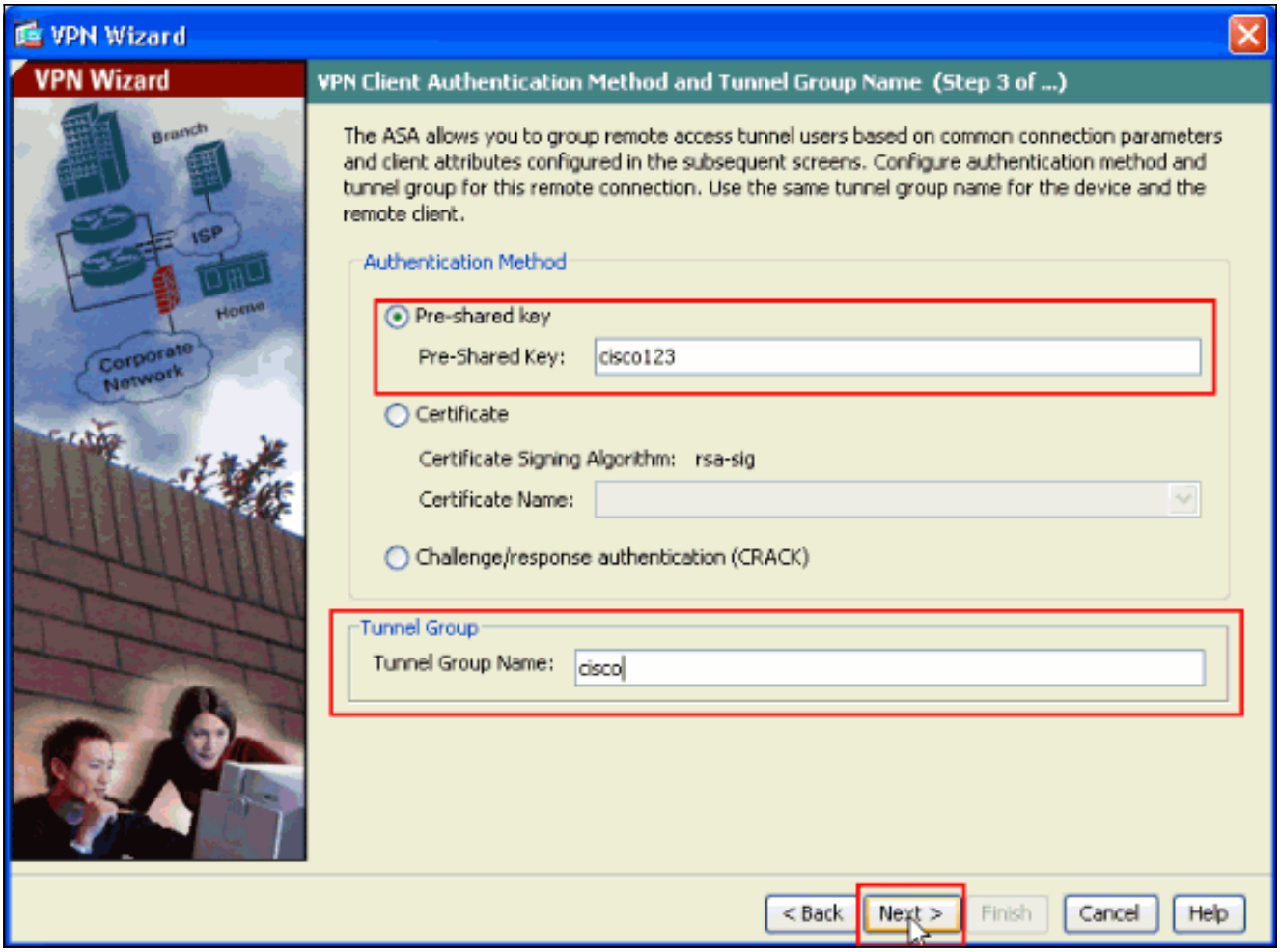
7. 표시된 대로 VPN Client Type(VPN 클라이언트 유형)이 선택됩니다.**Cisco VPN Client**가 여기서 선택됩니다.Next(**다음)를 클릭합니다**

.

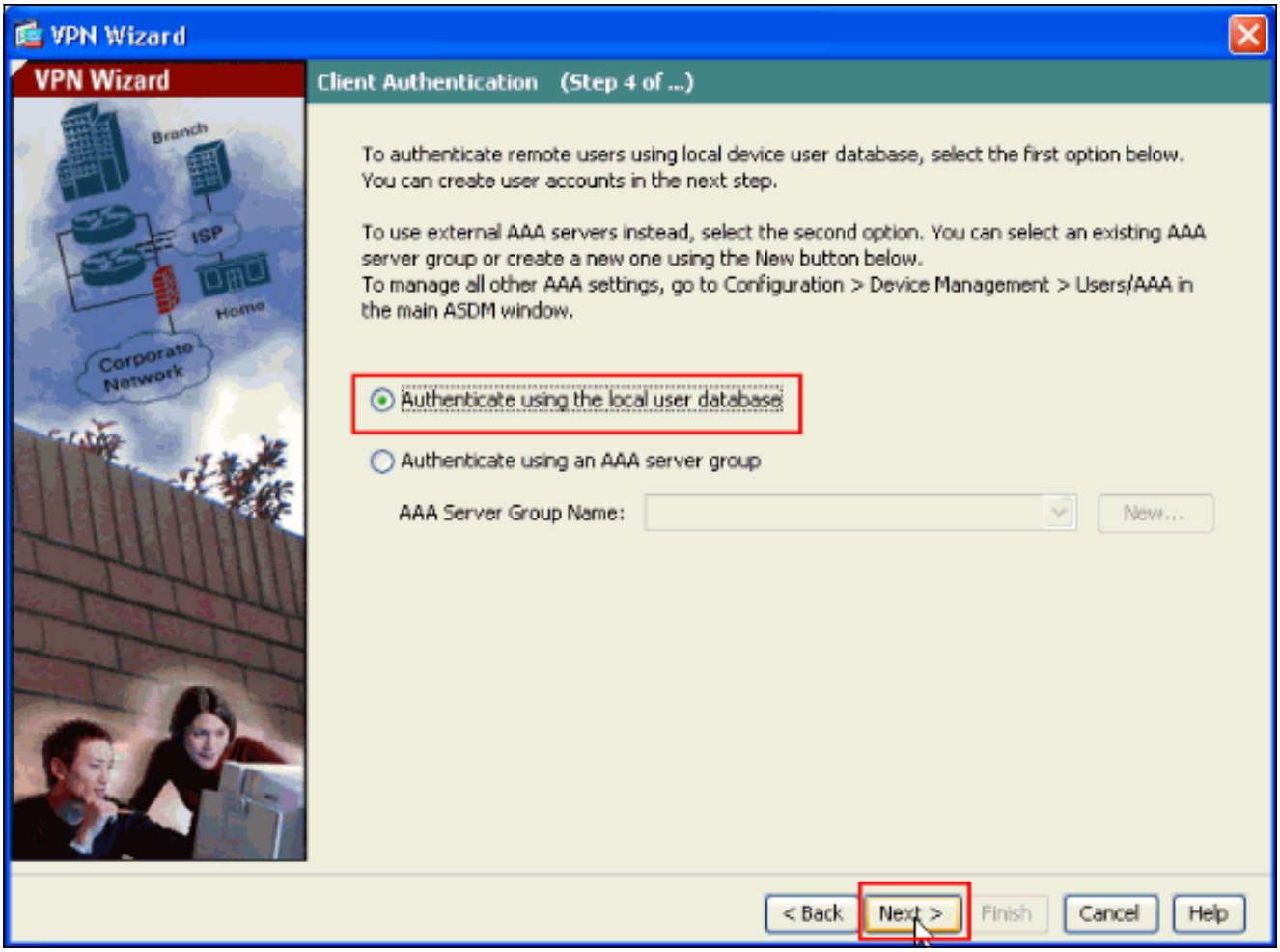


8. **터널 그룹 이름**의 이름을 **입력합니다**.사용할 인증 정보를 입력합니다. 이 정보는 이 예에서 **사전 공유 키입니다**.이 예에서 사용된 사전 공유 키는 **cisco123**입니다. 이 예에서 사용되는 터널 그룹 이름은 **cisco**입니다.Next(**다음)를 클릭합니다**

.

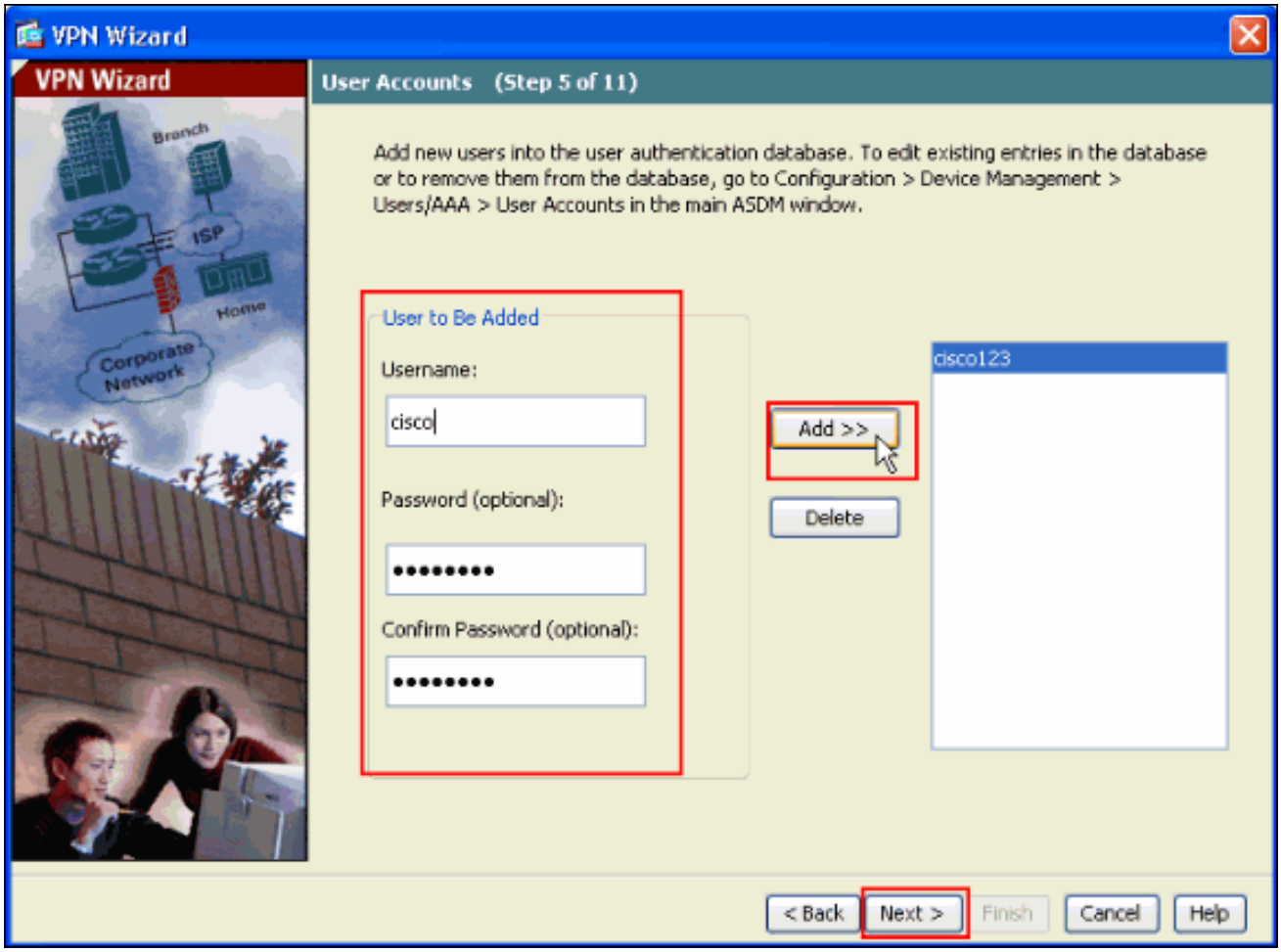


9. 원격 사용자를 로컬 사용자 데이터베이스에 인증할지 아니면 외부 AAA 서버 그룹에 인증할지를 선택합니다.**참고:** 10단계에서 사용자를 로컬 사용자 데이터베이스에 추가합니다.**참고:** ASDM을 사용하여 외부 AAA 서버 그룹을 구성하는 방법에 대한 자세한 내용은 ASDM 컨피그레이션을 통해 VPN 사용자용 PIX/ASA 7.x 인증 및 권한 부여 서버 그룹을 참조하십시오
.



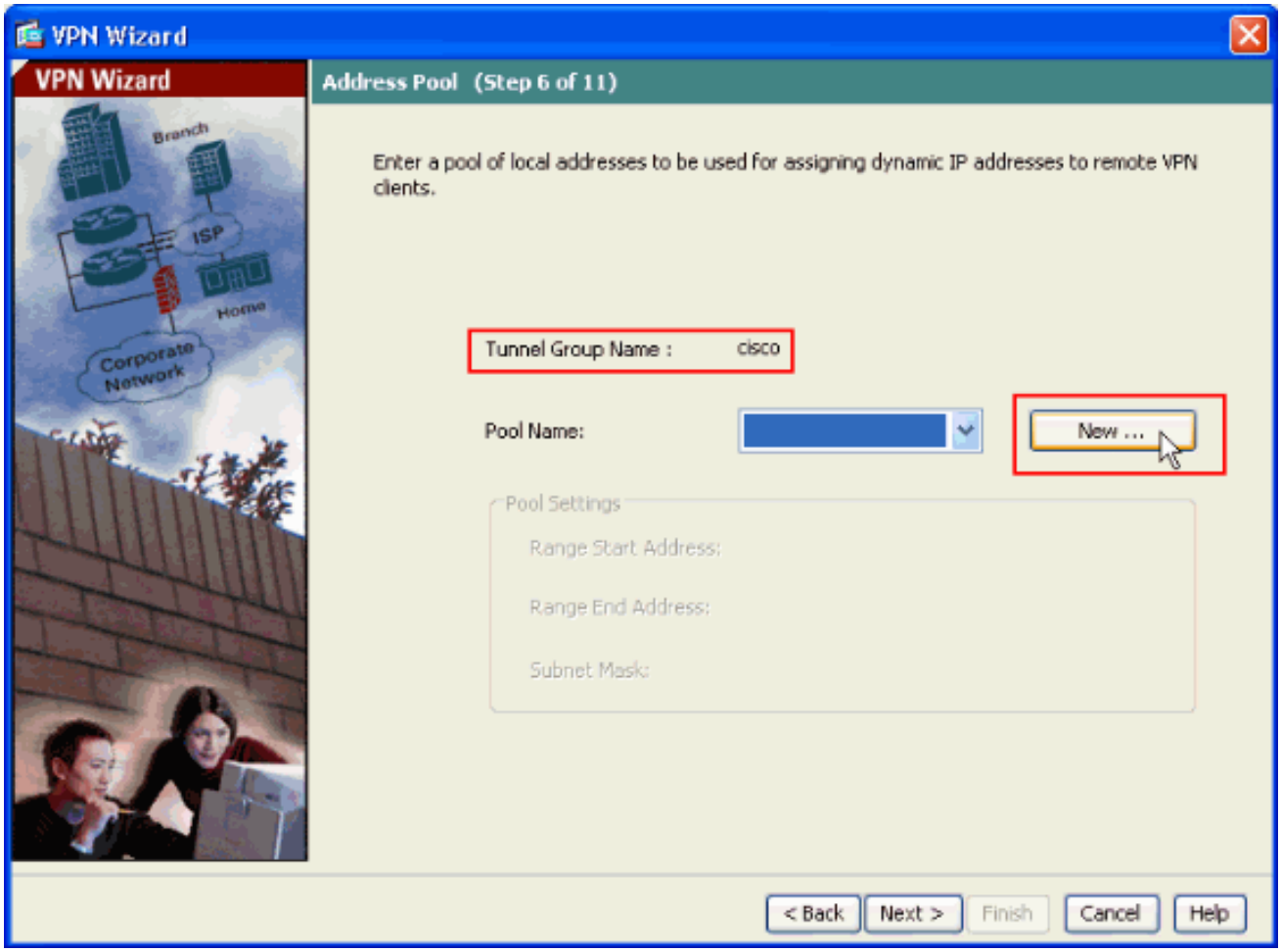
10. 사용자 **이름** 및 선택적 **비밀번호**를 **제공하고** Add를 클릭하여 사용자 인증 데이터베이스에 새 사용자를 추가합니다.Next(**다음)를 클릭합니다.참고:** 이 창에서 기존 사용자를 제거하지 마십시오.기본 ASDM 창**에서 Configuration > Device Management > Users/AAA > User Accounts**를 선택하여 데이터베이스의 기존 항목을 편집하거나 데이터베이스에서 제거합니다

.

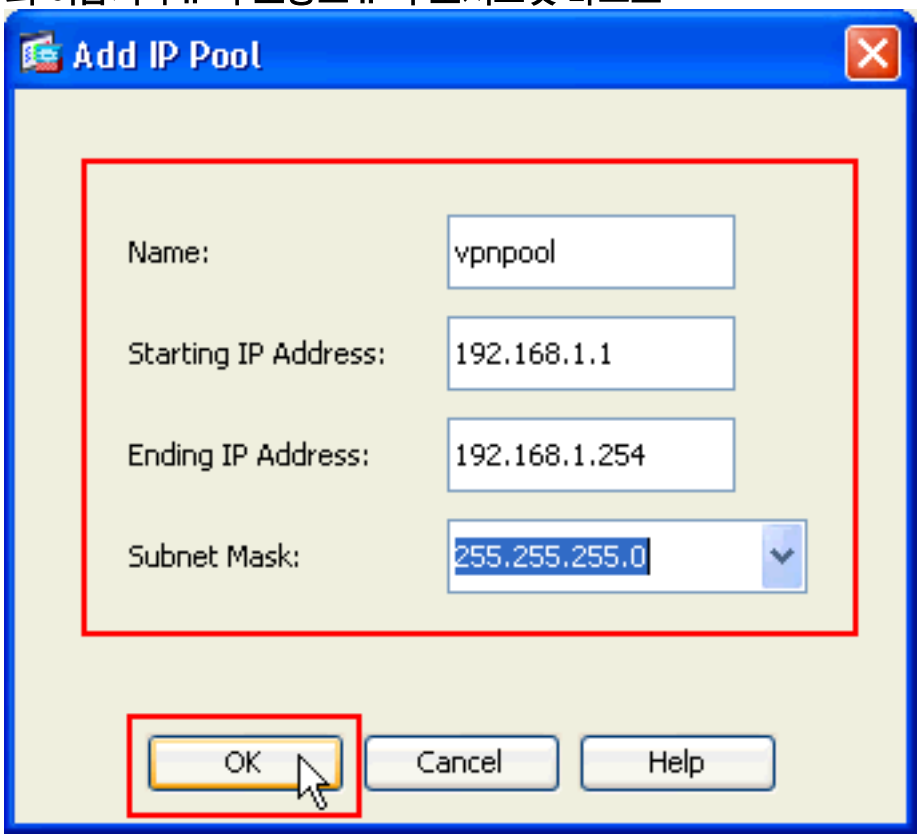


11. 원격 VPN 클라이언트에 동적으로 할당할 로컬 주소 풀을 정의하려면 **New**(새로 만들기)를 클릭하여 새 **IP 풀**을 **생성합니다**

.

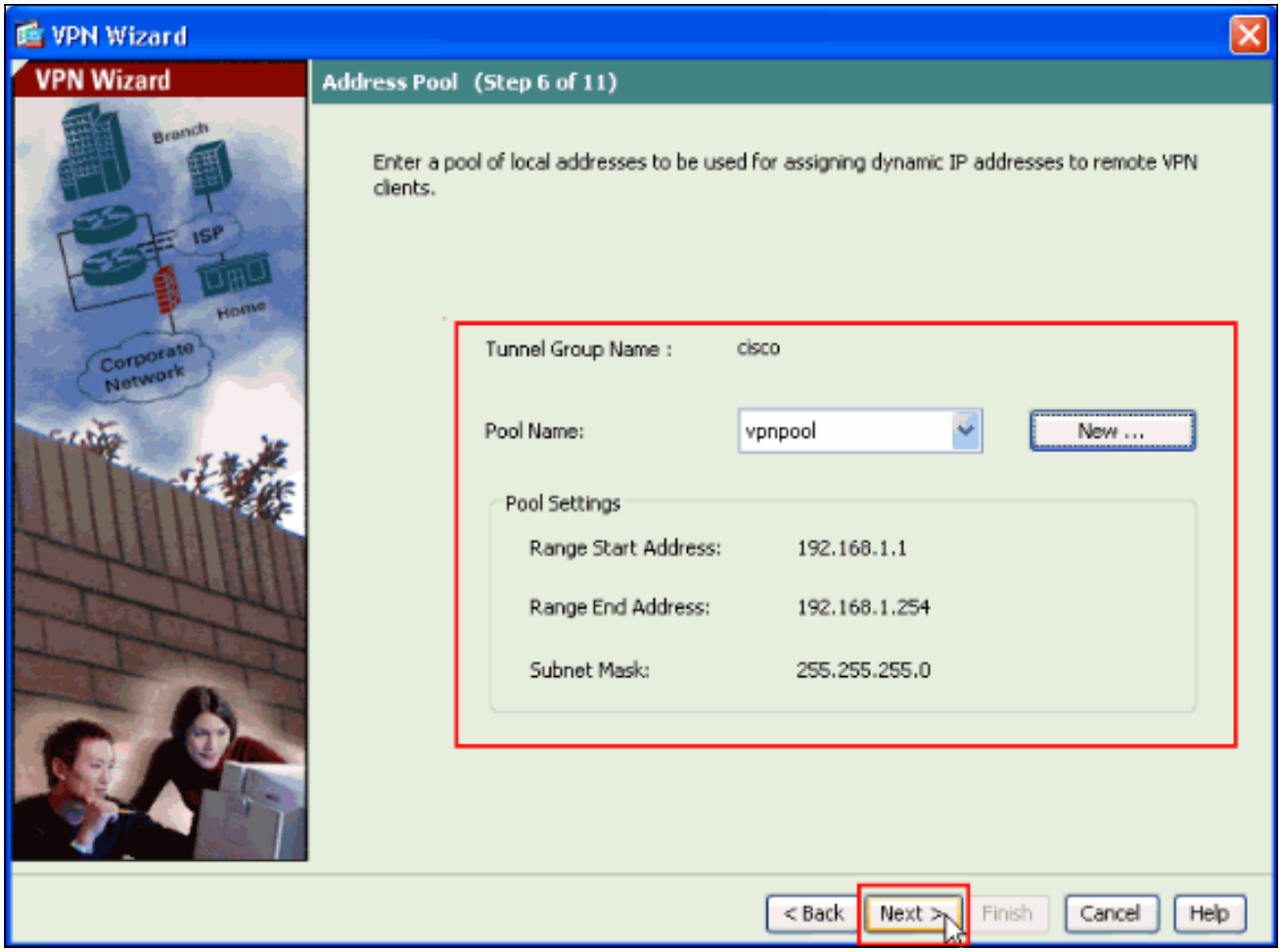


12. Add **IP Pool(IP 풀 추가)**이라는 새 창에서 이 정보를 제공하고 **OK(확인)**를 클릭합니다.**IP 풀의 이름시작 IP 주소종료 IP 주소서브넷 마스크**



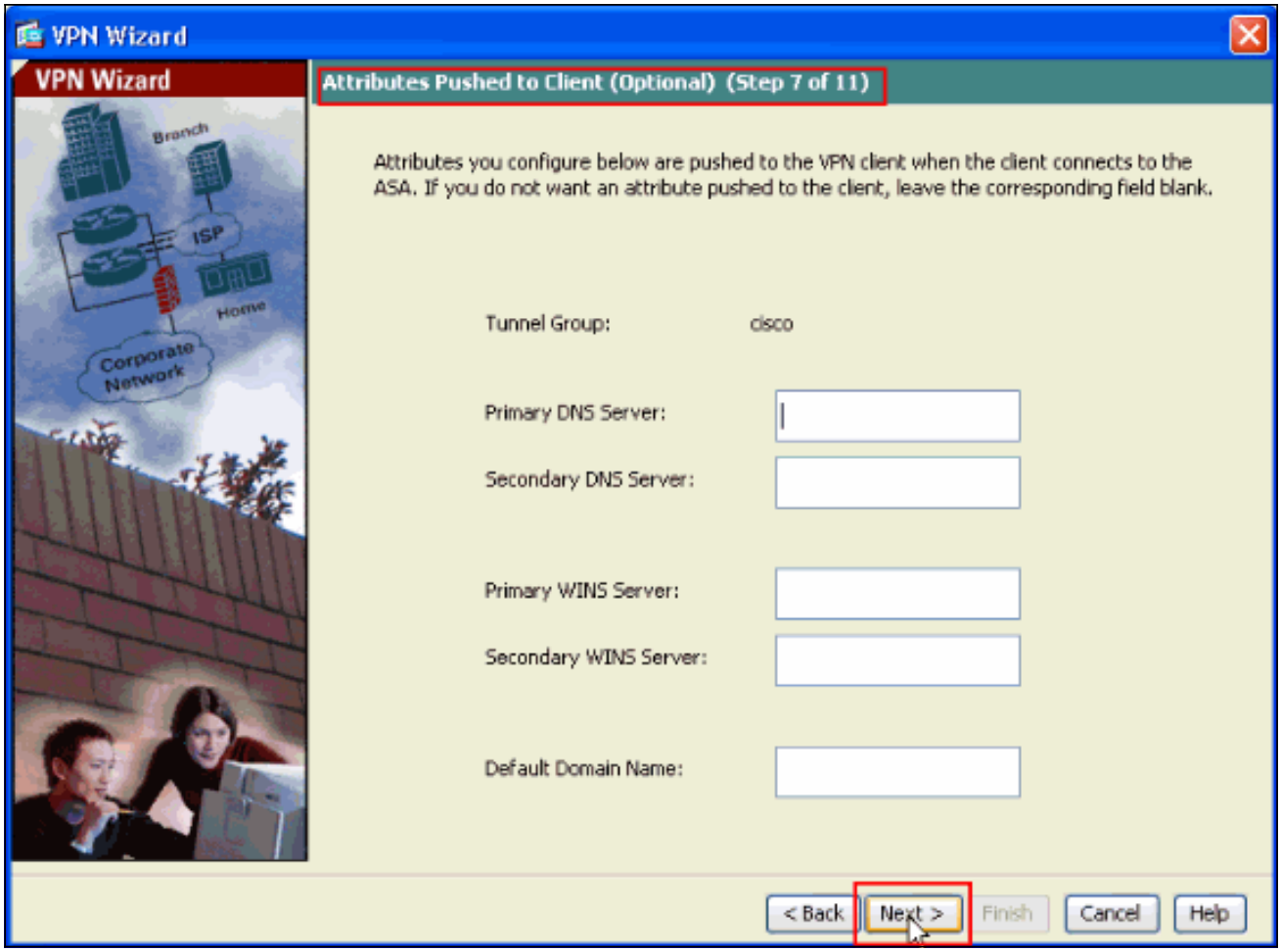
13. 연결할 때 원격 VPN 클라이언트에 동적으로 할당할 로컬 주소의 풀을 정의한 후 Next(**다음**)를 클릭합니다

.

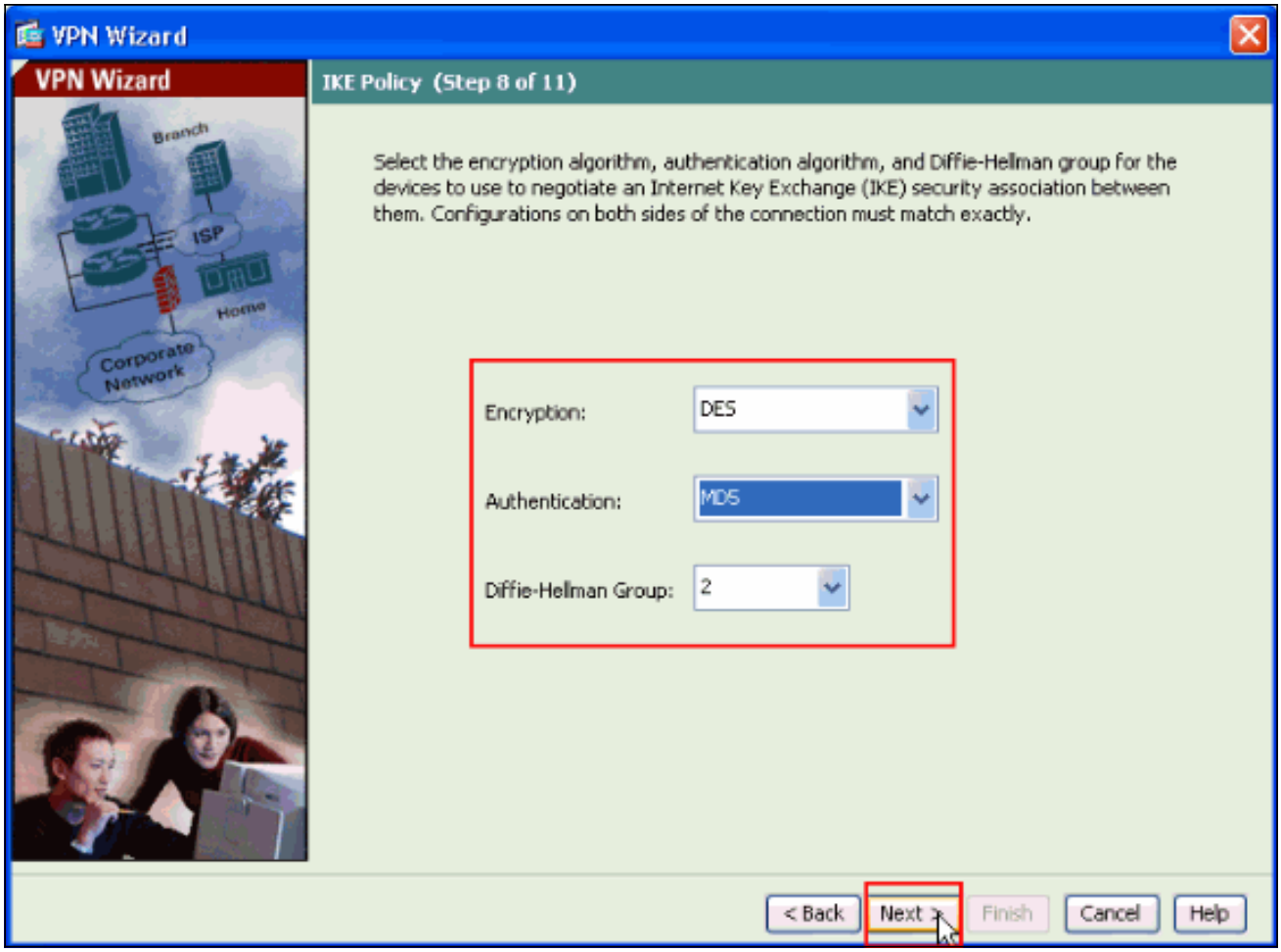


14. *선택 사항:*원격 VPN 클라이언트에 푸시할 DNS 및 WINS 서버 정보 및 기본 도메인 이름을 지정합니다

.

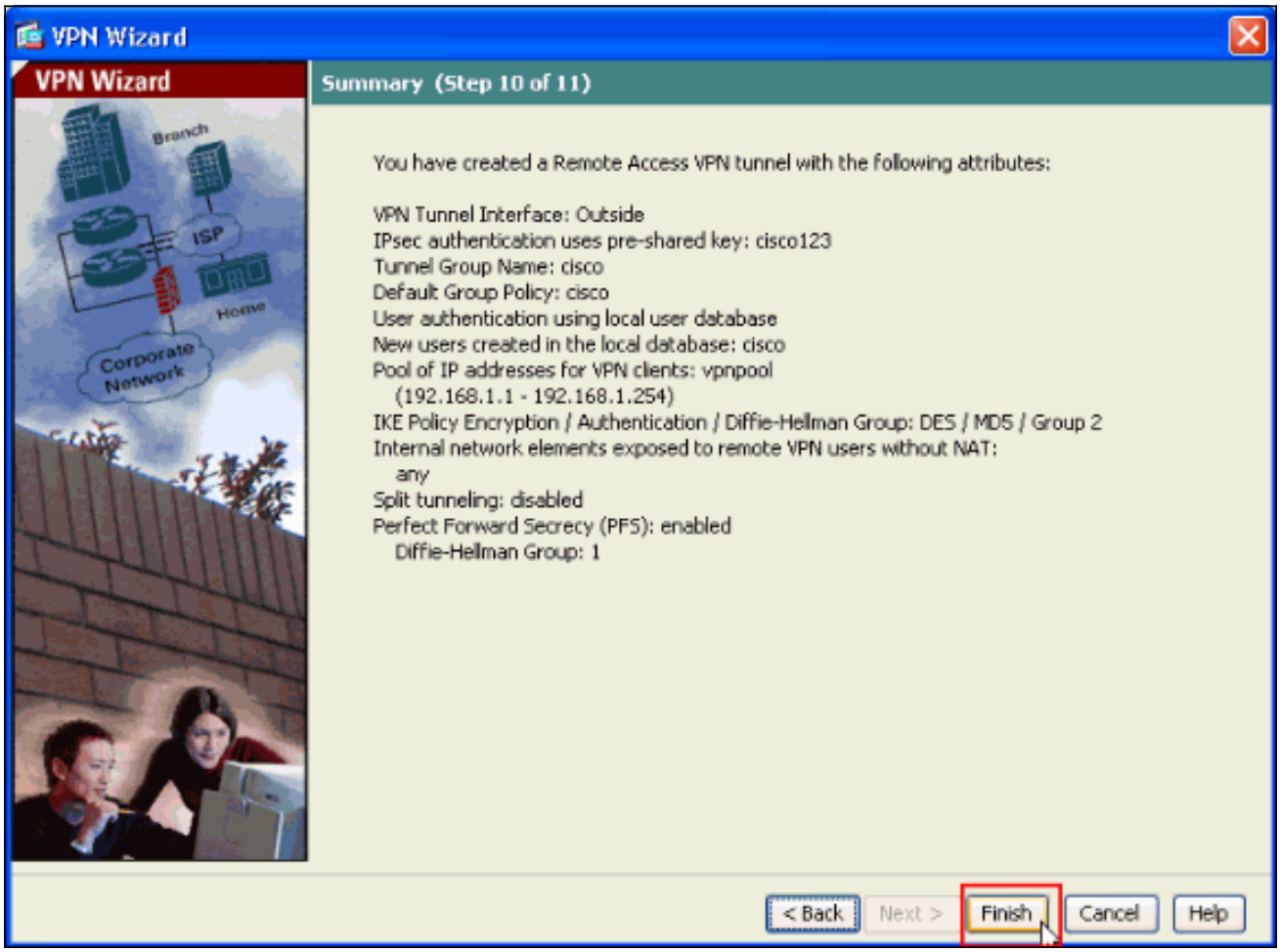


15. IKE 1단계라고도 하는 IKE의 매개변수를 지정합니다.터널의 양쪽에 있는 컨피그레이션은 정확히 일치해야 합니다.그러나 Cisco VPN Client는 자동으로 자신에게 적합한 컨피그레이션을 선택합니다.따라서 클라이언트 PC에는 IKE 컨피그레이션이 필요하지 않습니다
.



16. 이 창에는 수행한 작업의 요약이 표시됩니다.구성에 만족하면 마침을 클릭합니다

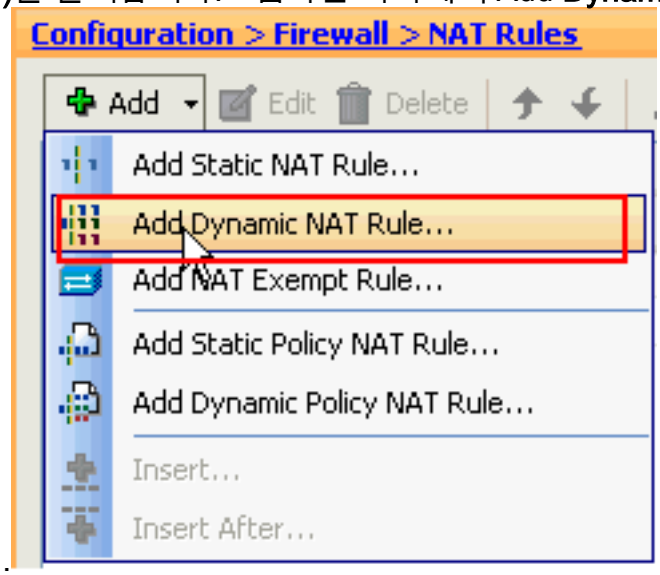
.



ASDM을 사용하여 NAT 인바운드 VPN 클라이언트 트래픽에 ASA/PIX 구성

ASDM을 사용하여 Cisco ASA-NAT 인바운드 VPN 클라이언트 트래픽을 구성하려면 다음 단계를 완료합니다.

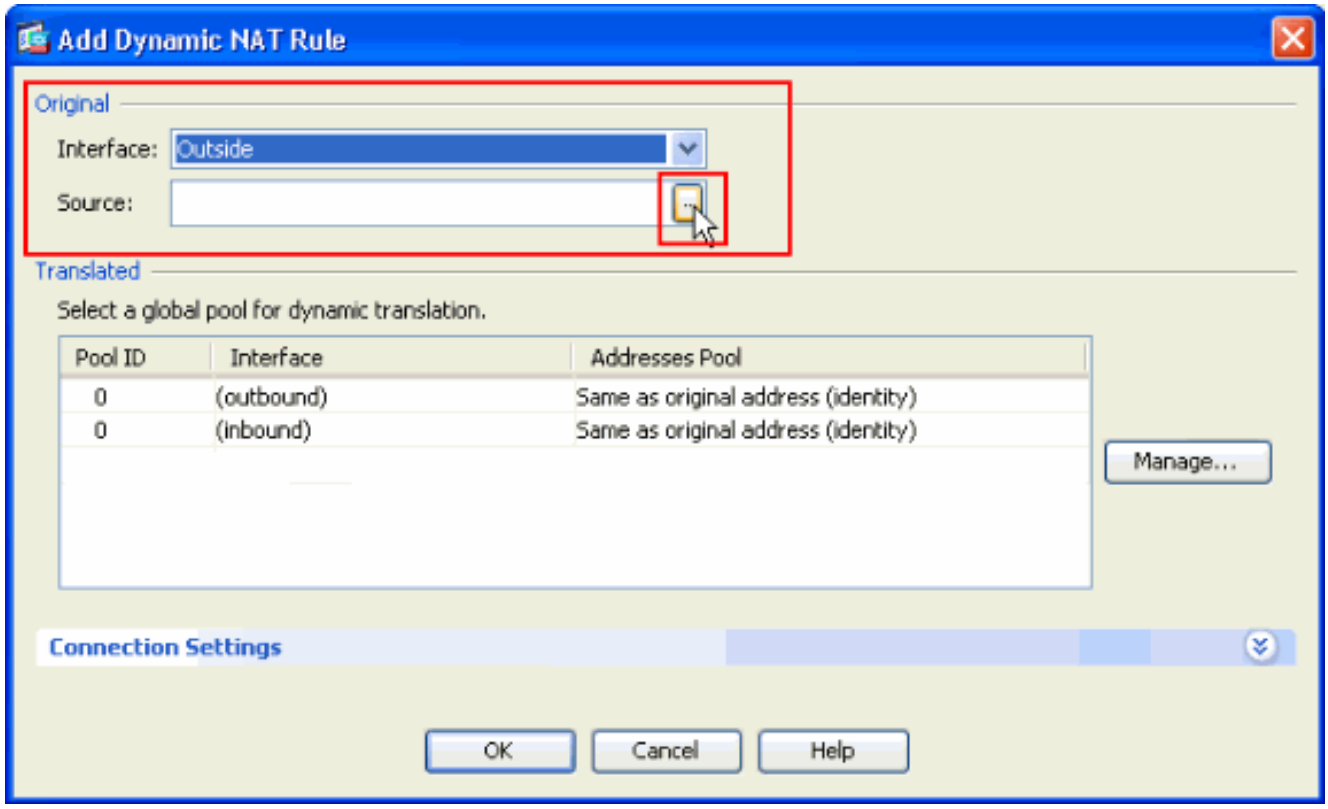
1. Configuration(**컨피그레이션) > Firewall(방화벽) > Nat Rules**(NAT 규칙)를 선택하고 **Add(추가**)를 클릭합니다.드롭다운 목록에서 Add **Dynamic NAT Rule을** 선택합니다



.

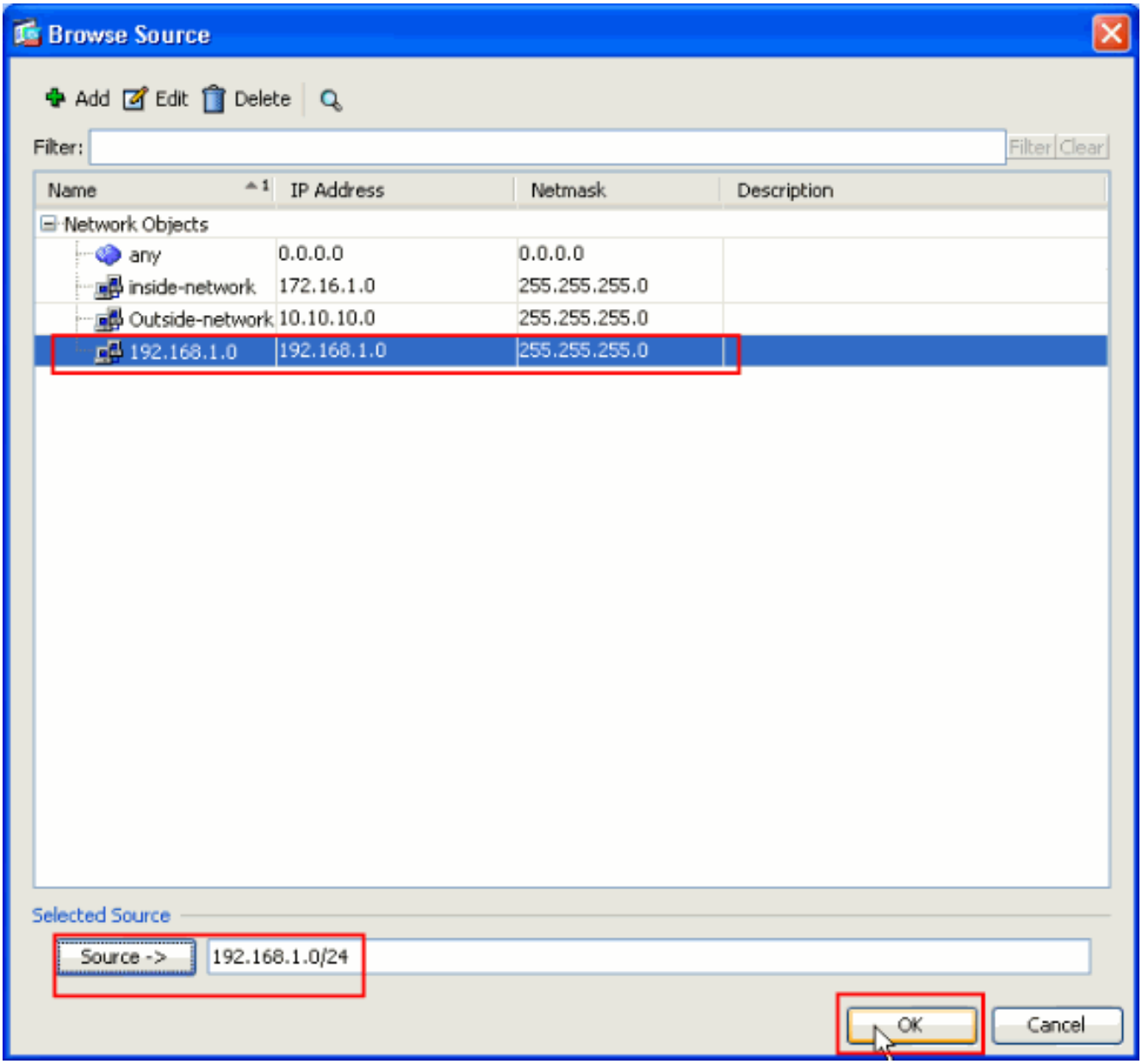
2. Add **Dynamic NAT Rule(동적 NAT 규칙 추가**) 창에서 **Outside(외부**)를 Interface(인터페이스)로 선택하고 Source(소스) 상자 옆에 있는 찾아보기 버튼을 클릭합니다

.



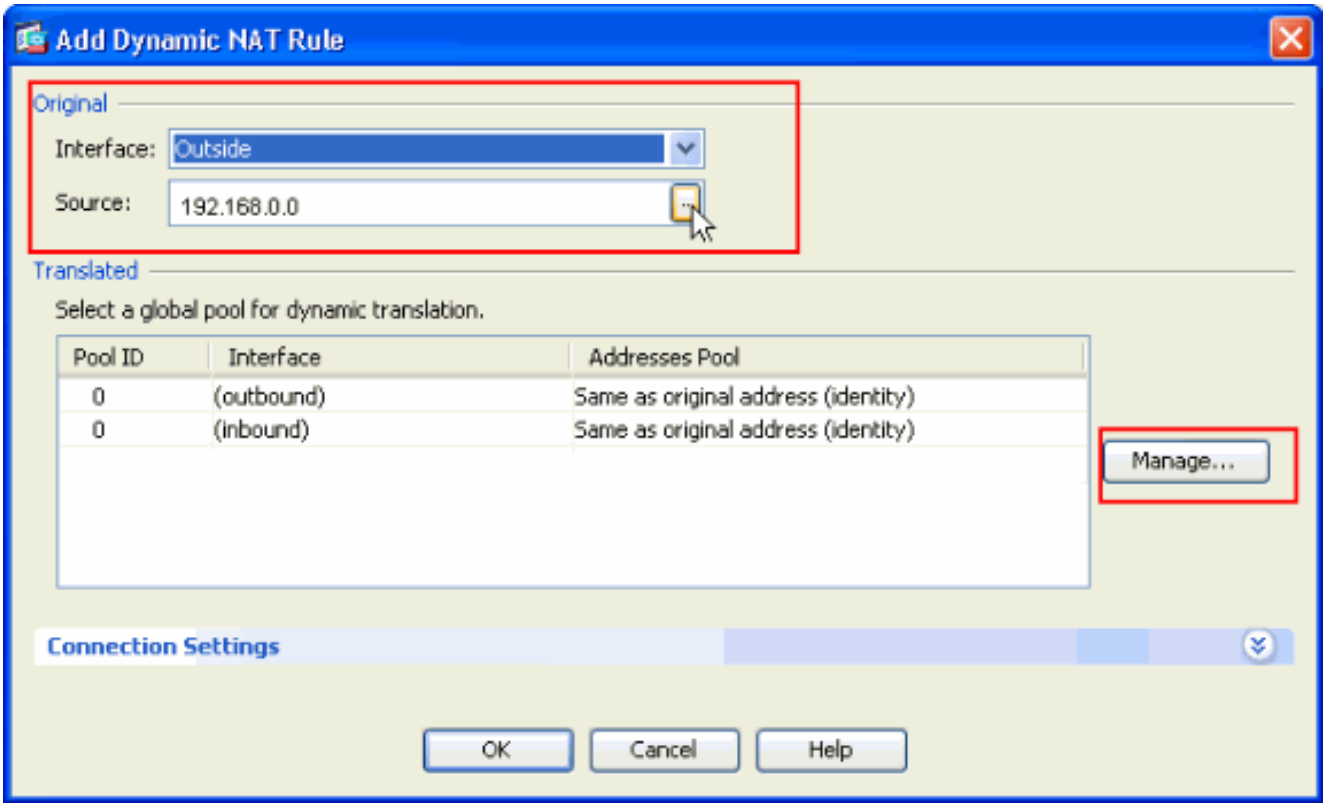
3. Browse Source(소스 찾아보기) 창에서 적절한 네트워크 객체를 선택하고 Selected Source(선택한 소스) 섹션 아래에서 **소스**를 선택하고 **OK(확인)**를 클릭합니다.여기서 192.168.1.0 네트워크 객체가 선택됩니다

.

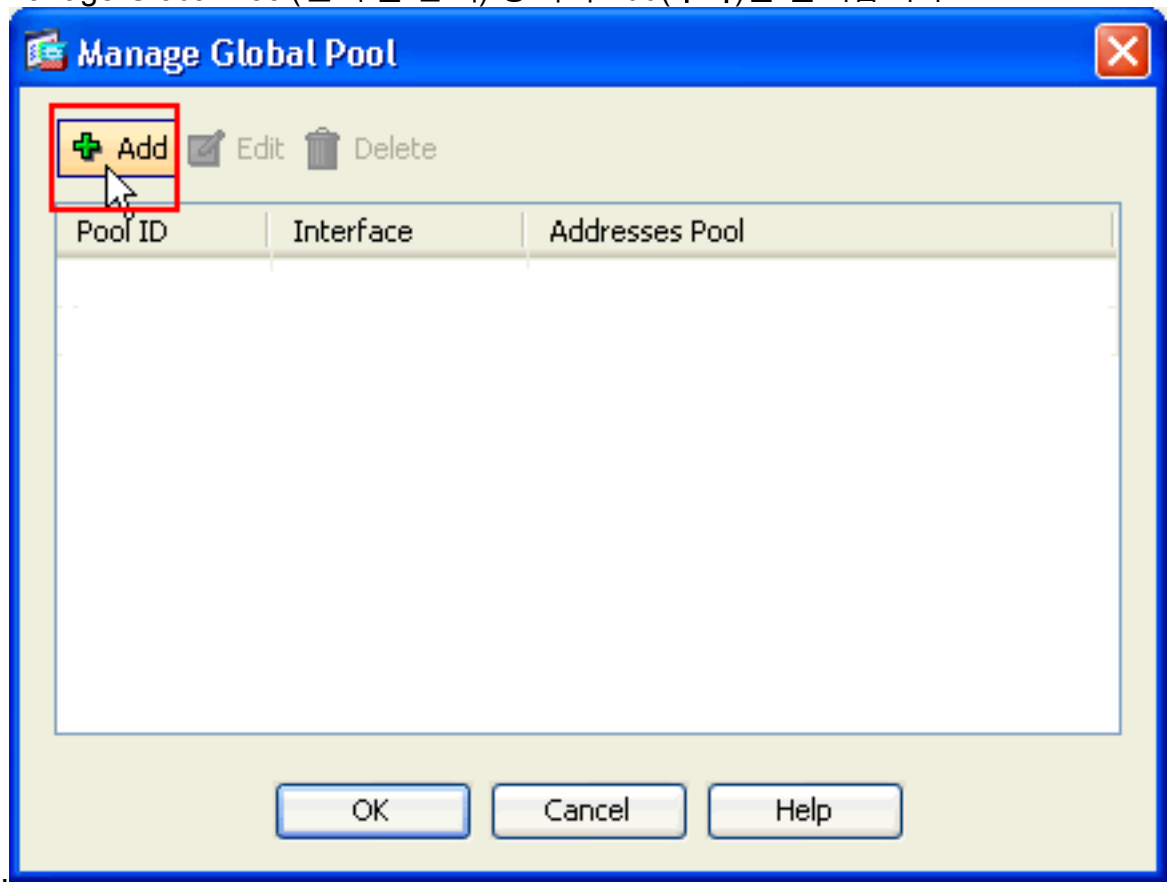


4. Manage(관리)를 클릭합니다

.



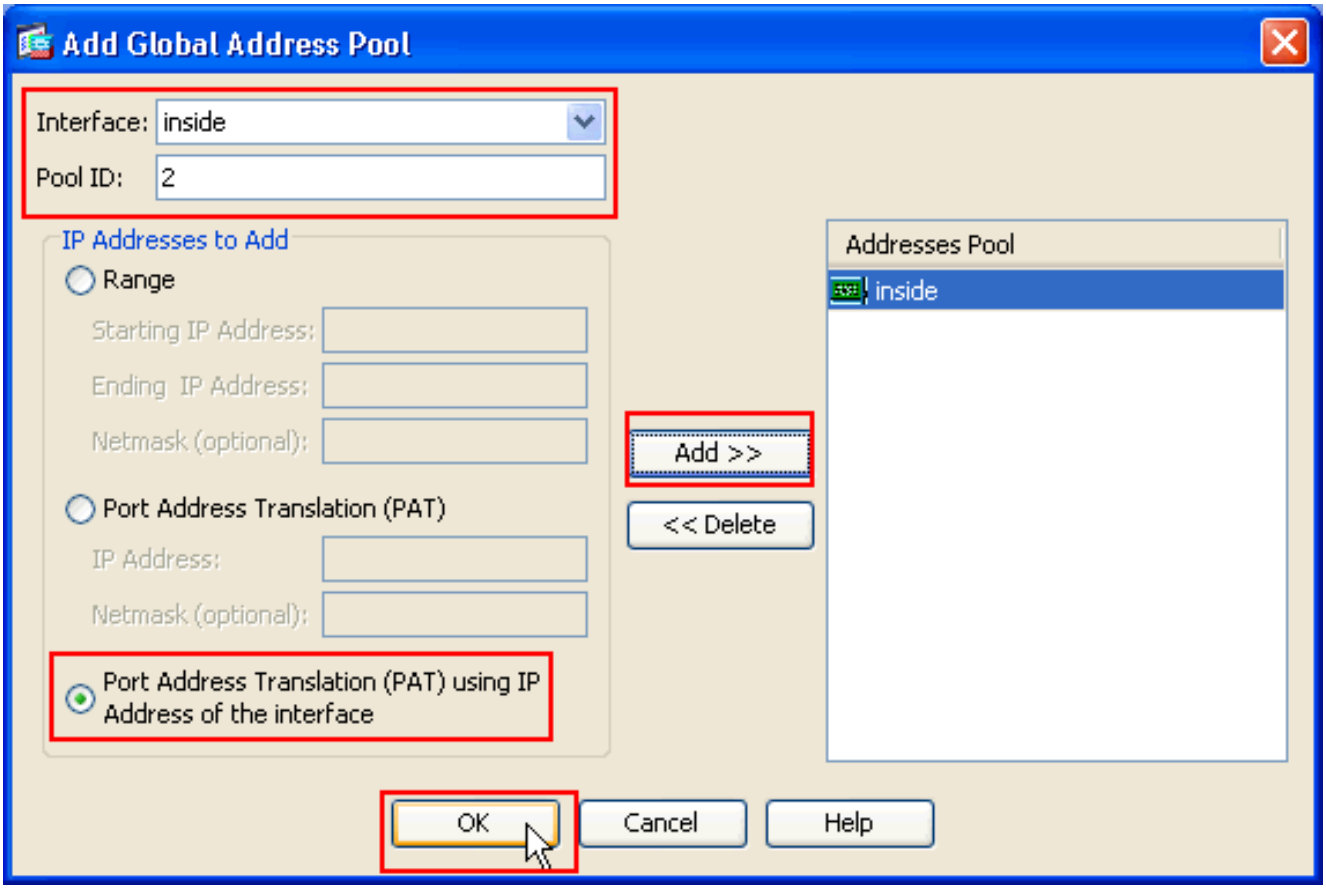
5. Manage Global Pool(전역 풀 관리) 창에서 Add(**추가**)를 클릭합니다



.

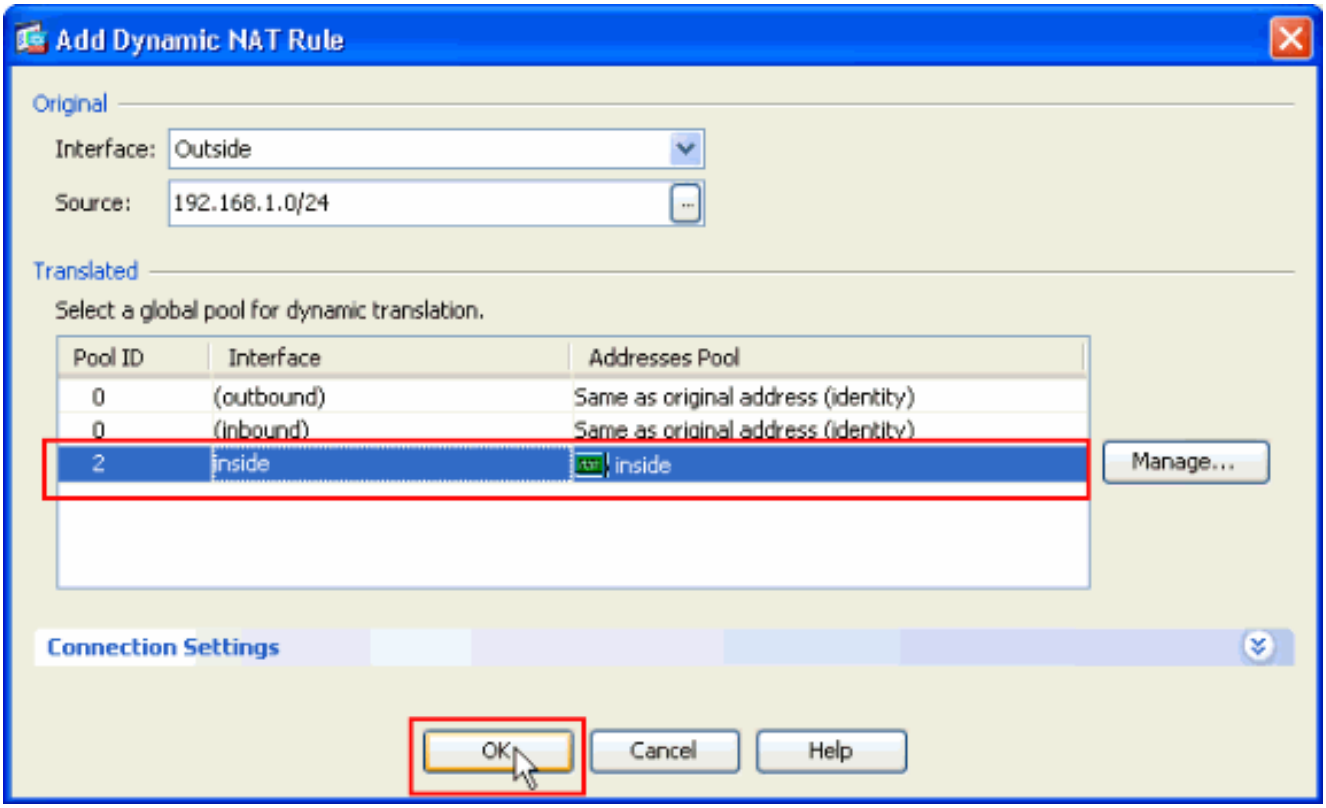
6. Add Global Address Pool(전역 주소 풀 추가) 창에서 **Inside**를 인터페이스로, **2**를 **풀 ID로** 선택합니다.또한 **인터페이스**의 **IP 주소**를 **사용하는 PAT** 옆의 라디오 버튼**이** 선택되었는지 확인합니다.Add(**추가)>>**를 클릭한 다음 **OK(확인)**를 클릭합니다

.



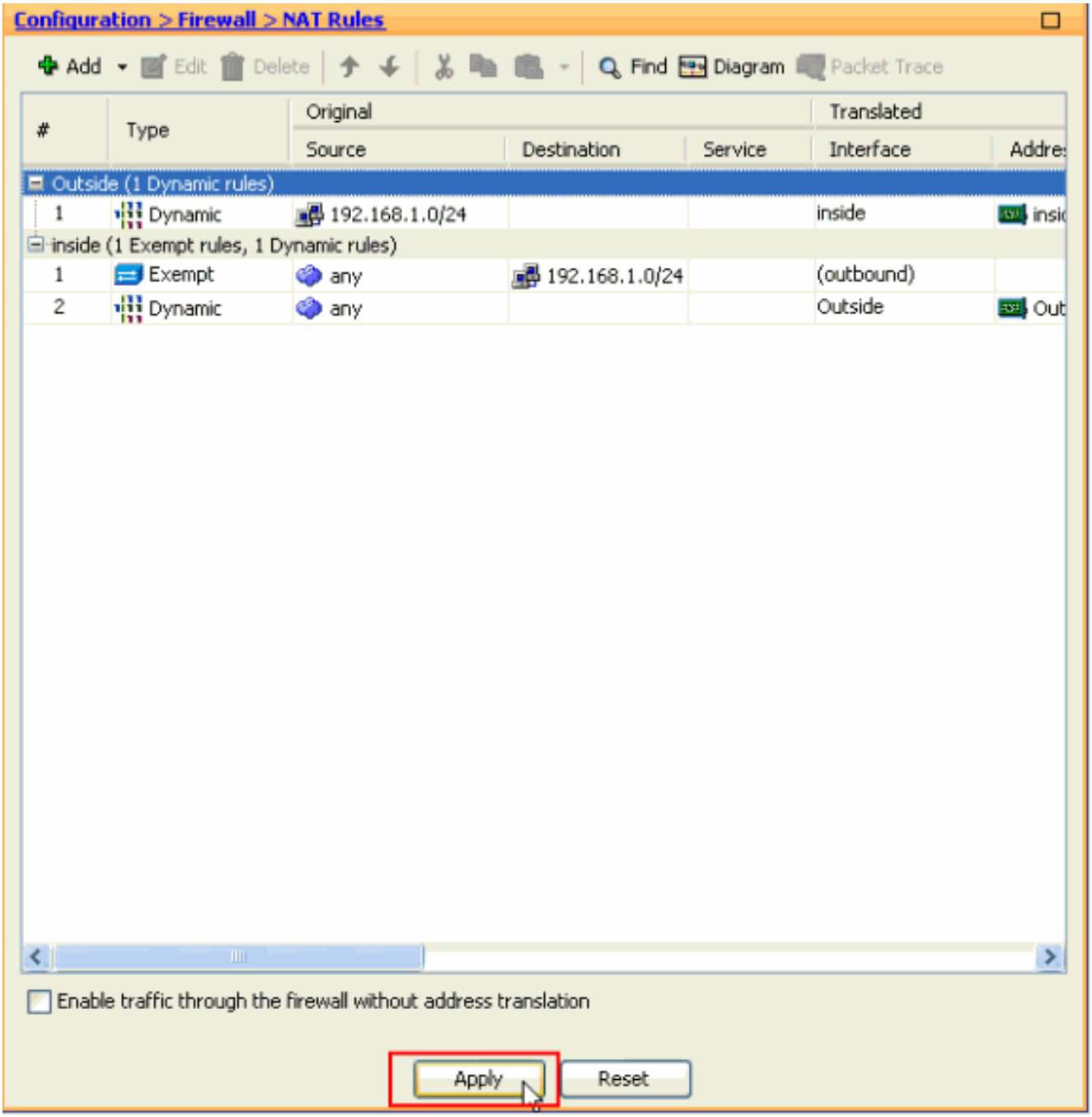
7. 이전 단계에서 **풀 ID 2**가 구성된 전역 풀을 선택한 후 OK(확인)를 클릭합니다

.



8. 이제 **Apply(적용)**를 클릭하여 컨피그레이션이 ASA에 적용되도록 합니다.이렇게 하면 컨피그레이션이 완료됩니다

.



[ASA/PIX를 원격 VPN 서버로 구성하고 CLI를 사용하여 인바운드 NAT를 구성합니다 .]

ASA 디바이스에서 컨피그레이션 실행
ciscoasa#**show running-config** : Saved ASA Version 8.0(3) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 10.10.10.2 255.255.255.0

```
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa803-k8.bin
ftp mode passive
access-list inside_nat0_outbound extended permit ip any
192.168.1.0 255.255.255
0
pager lines 24
logging enable
mtu Outside 1500
mtu inside 1500
ip local pool vpnpool 192.168.1.1-192.168.1.254 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
asdm history enable
arp timeout 14400
nat-control
global (Outside) 1 interface
global (inside) 2 interface
nat (Outside) 2 192.168.1.0 255.255.255.0 outside
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
no snmp-server location
no snmp-server contact

!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ESP-DES-
SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-
hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
transform-set ESP-DES-SH
 ESP-DES-MD5
crypto map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
crypto map Outside_map interface Outside
crypto isakmp enable Outside

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
```

```
used during an IKE negotiation. Encryption and !---
Policy details are hidden as the default values are
chosen. crypto isakmp policy 10
authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 30
 authentication pre-share
 encryption des
 hash md5
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 60
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
group-policy cisco internal
group-policy cisco attributes
 vpn-tunnel-protocol IPSec

!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 0

username cisco attributes
 vpn-group-policy cisco
tunnel-group cisco type remote-access
tunnel-group cisco general-attributes
 address-pool vpnpool
 default-group-policy cisco

!--- Specifies the pre-shared key "cisco123" which must
!--- be identical at both peers. This is a global !---
configuration mode command. tunnel-group cisco ipsec-
attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
```

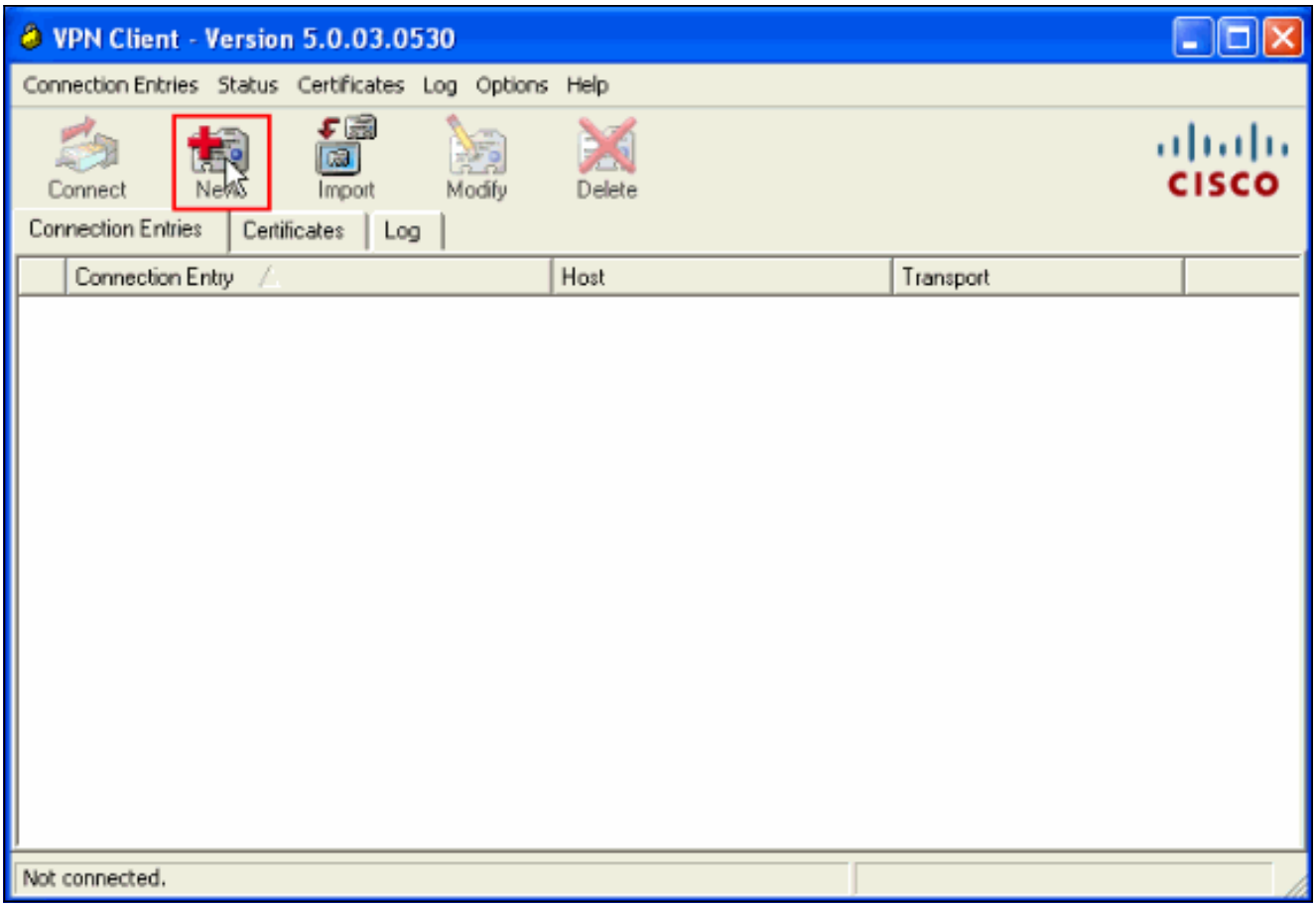
```
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3
: end
ciscoasa#
```

다음을 확인합니다.

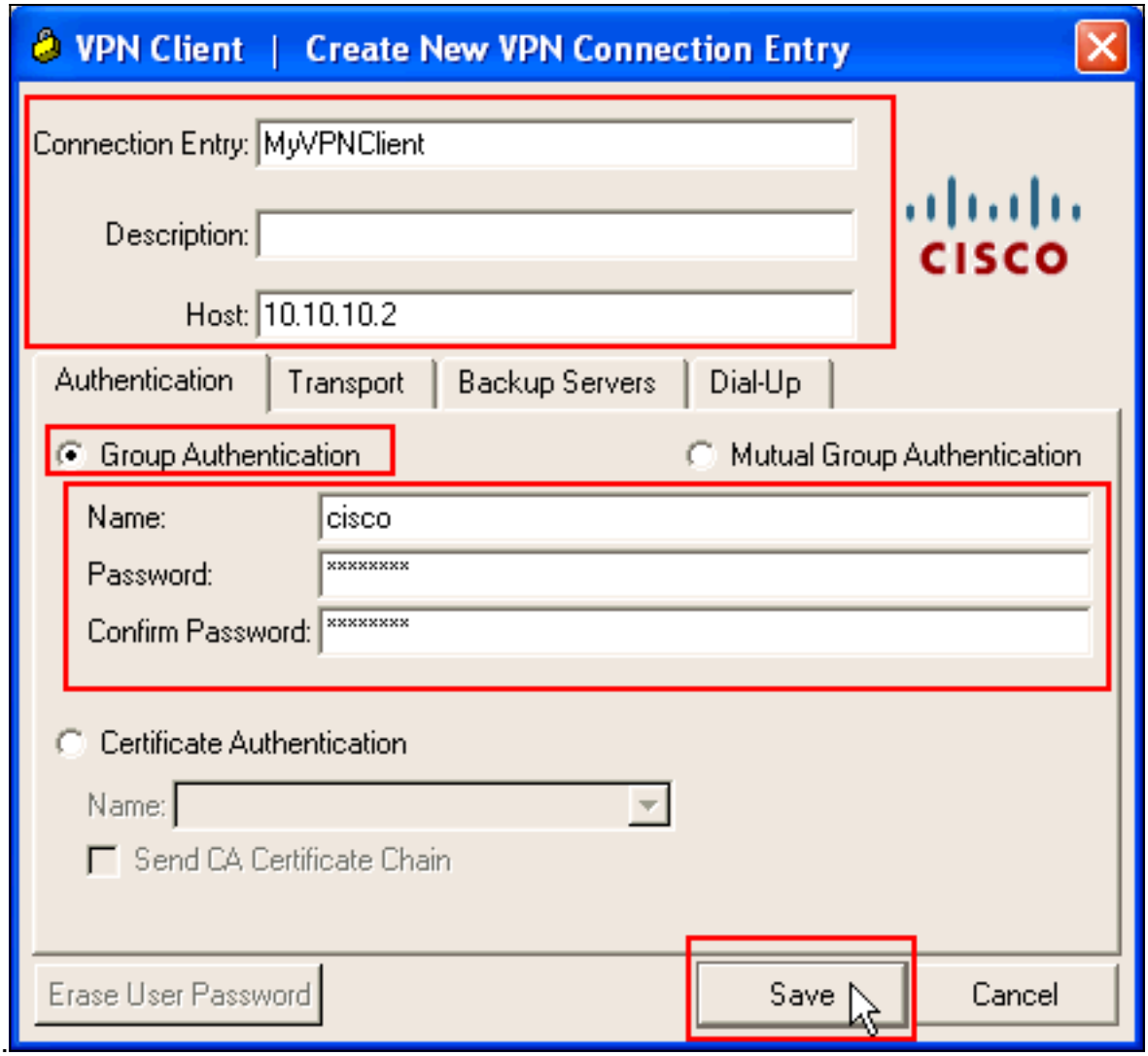
ASA가 성공적으로 구성되었는지 확인하기 위해 Cisco VPN 클라이언트를 통해 Cisco ASA에 연결하려고 시도합니다.

1. New(**새로 만들기**)를 클릭합니다

.

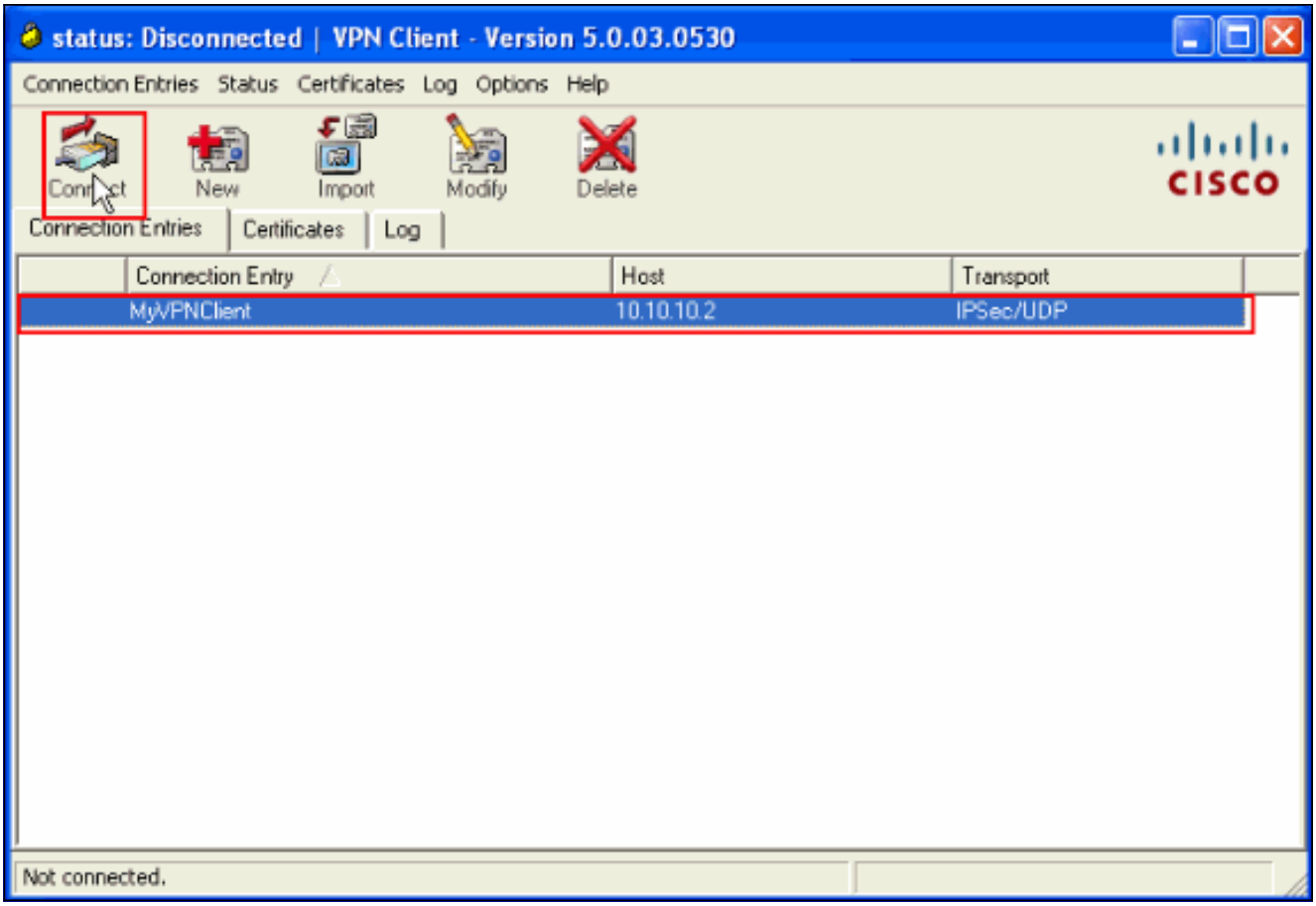


2. 새 연결의 세부 정보를 입력합니다.Host 필드에는 이전에 구성한 Cisco ASA의 IP 주소 또는 호스트 이름이 포함되어야 합니다.그룹 인증 정보는 **4단계**에서 사용된 것과 일치해야 합니다. 완료되면 저장을 클릭합니다



3. 새로 생성된 연결을 선택하고 **연결**을 클릭합니다

.

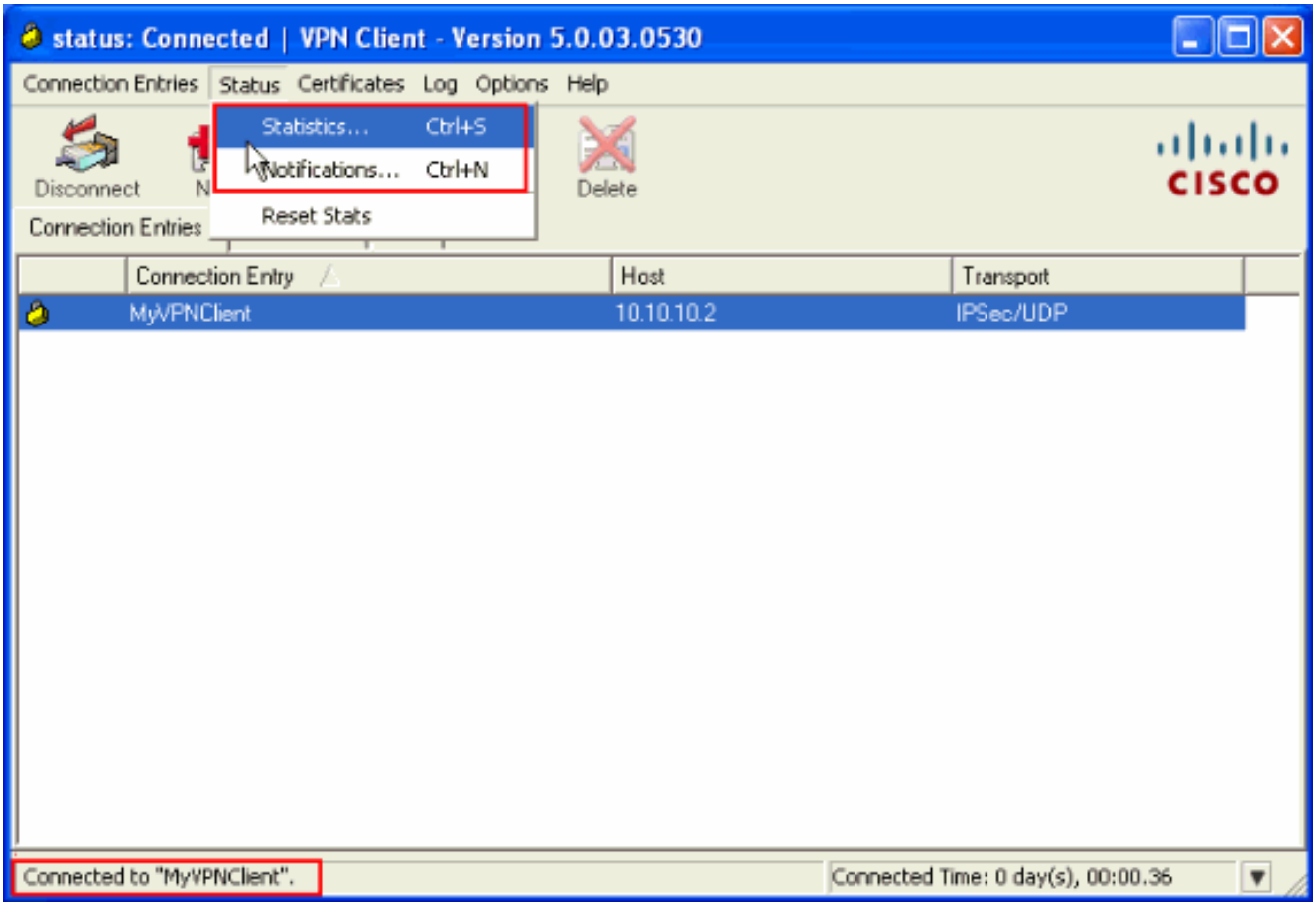


4. 확장 인증을 위한 사용자 이름 및 비밀번호를 입력합니다.이 정보는 **5단계 및 6단계**에 지정된 정보와 일치해야 합니다

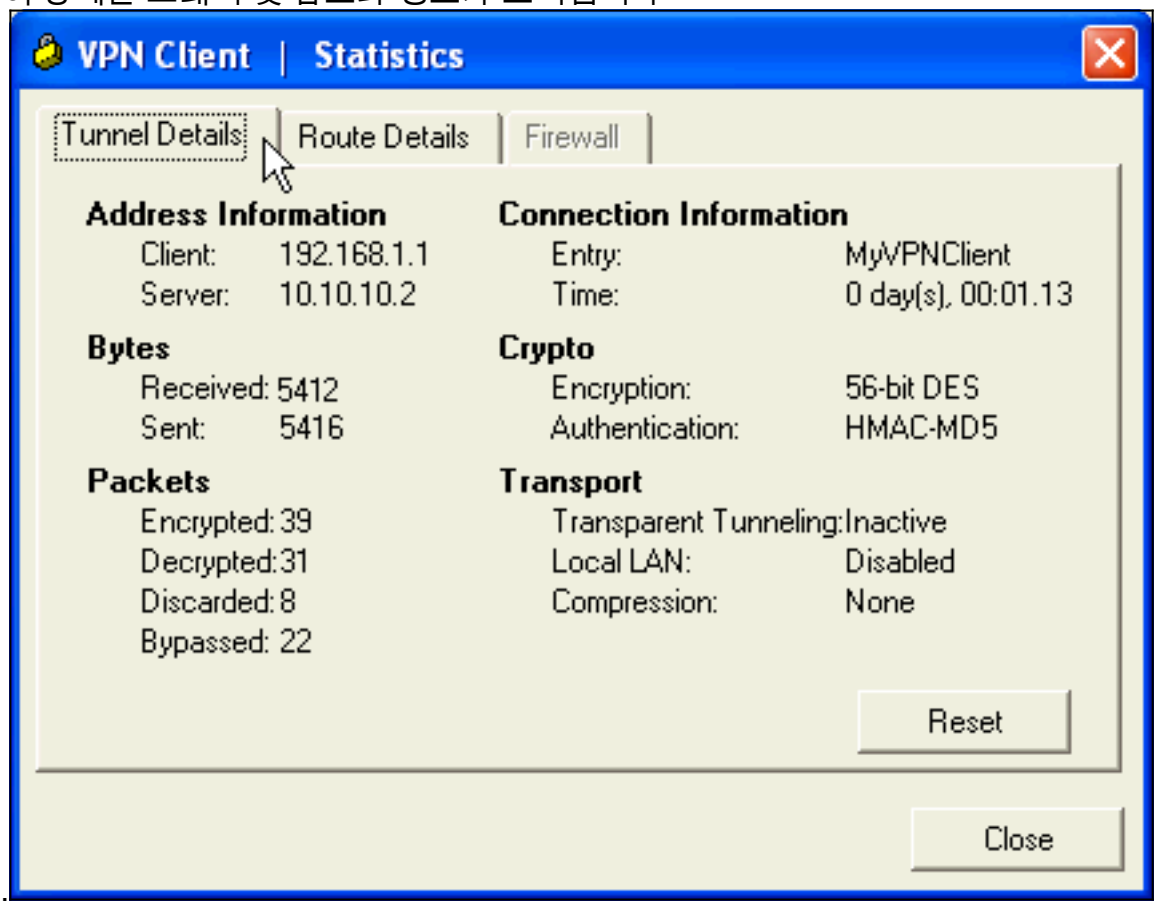
.

5. 연결이 성공적으로 설정되면 Status 메뉴에서 Statistics를 선택하여 터널의 세부 정보를 확인합니다

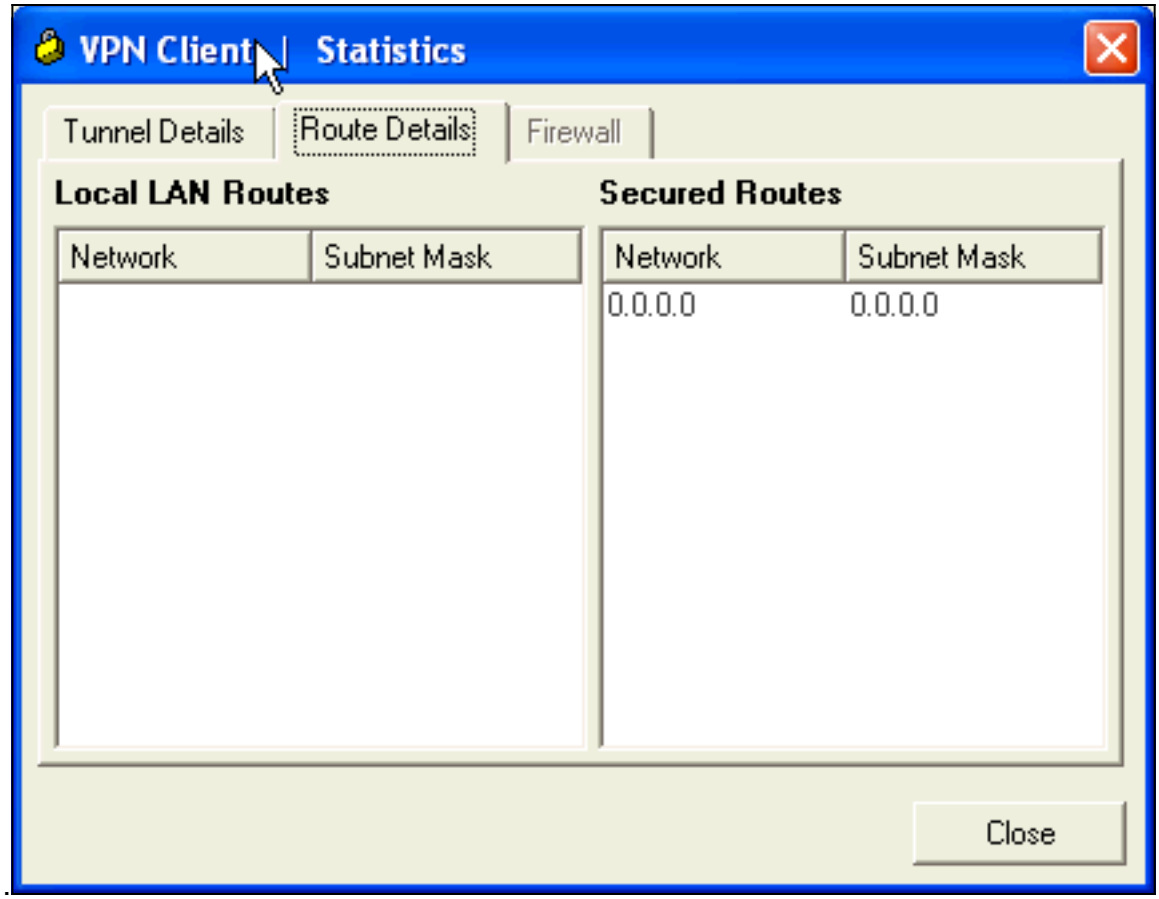
.



이 창에는 트래픽 및 암호화 정보가 표시됩니다



.이 창에는 스플릿 터널링 정보가 표시됩니다



ASA/PIX Security Appliance - show 명령

- **show crypto isakmp sa** - 피어의 현재 IKE SA를 모두 표시합니다.

```
ASA#show crypto isakmp sa

      Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.10.10.1
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
```

- **show crypto ipsec sa** - 피어에 있는 모든 현재 IPsec SA를 표시합니다.

```
ASA#show crypto ipsec sa
interface: Outside
    Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
.10.2

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
      current_peer: 10.10.10.1, username: cisco123
      dynamic allocated peer ip: 192.168.1.1

      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
      #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: F49F954C

    inbound esp sas:
      spi: 0x3C10F9DD (1007745501)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xF49F954C (4104099148)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
```

- ```
  ciscoasa(config)#debug icmp trace
  !--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
  translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
  ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
  2
  !--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
  untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
  ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
  len=32
  ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
  ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
  2
  ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
  ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
  ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
  ```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

사이트 사이트 VPN 문제 해결 방법에 대한 자세한 내용은 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션을 참조하십시오.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances 트러블슈팅 및 알림
- 기술 지원 및 문서 – Cisco Systems
  ```